REMARKS

By the present amendment, claims 1-3, 11, 23-25, 41, 45-47, 49 and 50 have been amended, and claims 52-53 have been added. No new matter has been added

Applicants note that the above amendments of the pending claims are supported by, for example, page 92, line 22 - page 98 line 7 of the specification and, for example, Fig. 12. In view of the above amendments and the following remarks, reconsideration of the rejections and further examination are requested.

I. Objection to the Claims

Claims 1-3, 9, 11, 23-25, 41 and 45 have been objected to due to minor informalities. By the present amendment, Applicants have amended claims 1-3, 9, 11, 23-25, 41 and 45 to replace the term "operable" with the term "configured", as suggested by the Examiner. Thus, Applicants respectfully request that the Examiner withdraw the above-noted objection.

II. Claim Rejections under 35 U.S.C. §103

A. The Examiner has rejected claims 1, 3, 4, 24, 46, 47, 49 and 50 under 35 U.S.C §103(a) as being unpatentable over Gennaro et al. (US 5,937,066) in view of Gennaro et al. (US 5,907,618).

This rejection is respectfully traversed and submitted to be inapplicable to the pending claims for the following reasons.

The pending claims generally relate to a key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus. The shared-key generation apparatus generates a seed value, and generates a verification value and a shared key from the seed value. The shared-key generation apparatus also encrypts the

verification value to generate first encryption information, and encrypts the seed value based on the verification value to generate second encryption information. The shared-key generation apparatus further transmits to the shared-key recovery apparatus the first encryption information and the second encryption information without transmitting to the shared-key recovery apparatus the generated shared-key. The shared-key recovery apparatus receives from the shared-key generation apparatus the first encryption information and the second encryption information. The shared-key recovery apparatus also decrypts the first encryption information to generate a first decryption verification value, and decrypts the second encryption information based on the first decryption verification value to generate a decryption seed value. The shared-key recovery apparatus further generates a second decryption verification value and a decryption shared key from the decryption seed value according to the same method as used in the first shared-key generating unit of the shared-key generation apparatus. The shared-key recovery apparatus judges whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value, and judges that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value. The shared-key generation apparatus is distinct from the shared-key recovery apparatus, and the first encryption information is distinct from the second encryption information.

Applicants respectfully submit that Gennaro et al. (US 5,937,066), Gennaro et al. (US 5,907,618) and Hoffstein et al. do not disclose or suggest such a combination of features.

Gennaro et al. (US 5,937,066) relates to a cryptographic key recovery system in which a sender establishes a secret value with a receiver. In phase 1, the sender (Alice) generates a key-generating value KG and encrypts the key-generating value KG with a public key of the recovery agent (col.17, lines 12-48 and Fig.9). In phase 2, the sender (Alice) generates a key-encrypting key and multiply encrypts a session key K with the set of the key-encrypting keys KK (col.17, line 49 - col.18, line 15 and Fig.10). The sender (Alice) transmits to the receiver (Bob) the encrypted key-generating value KG and the multiply encrypted session key K. In recovery phase, the receiver (Bob) decrypts the key-generating value KG, regenerates the key-encrypting key KK from the decrypted key-generating value KG, and recovers the session key K with the regenerated key-encrypting key KK (col.18, lines 16-30).

However, as the Examiner admitted in the Office Action dated on April 2, 2008, Gennaro et al. (US 5,937,066) fails to disclose at least a shared-key recovery apparatus that decrypts the first encryption information to generate a first decryption verification value, and decrypts the second encryption information based on the first decryption verification value to generate a decryption seed value, as well as a shared-key recovery apparatus that judges whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value, and judges that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value.

Thus, the pending claims are clearly distinguished over Gennaro et al. (US 5,937,066).

In the Office Action, however, the Examiner relies on Gennaro et al. (US 5,907,618) regarding that which the Examiner admits is lacking in Gennaro et al. (US 5,937,066). Gennaro et al. (US 5,907,618) relates to a method and apparatus for verifiably providing key recovery information to one or more trustees in a cryptographic communication system having a sender and a receiver. Each communication party has its own Diffie-Hellman key pair. The sender generates, from its own secret value and the public value held by the receiver, a first shared Diffie-Hellman key pair including a first shared value and the corresponding public key. The sender generates an additional shared secret value from the first shared secret value and the public value held by the trustee. The sender encrypts a session key K for each trustee using the additional shared secret value. The sender transmits the encrypted session key K to the receiver with the encrypted message. Each trustee regenerates its additional shared secret value from its own secret value and the public value of the Diffie-Hellman key pair to decrypt the session key K. The receiver verifies the correctness of the session key K for each trustee by decrypting the session key K, using the additional shared secret value for that trustee.

However, Gennaro et al. (US 5,907,618) fails to disclose at least a shared-key recovery apparatus that decrypts the first encryption information to generate a first decryption verification value, and decrypts the second encryption information based on the first decryption verification value to generate a decryption seed value, as well as a shared-key recovery apparatus that judges whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value, and judges that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the

first decryption verification value is identical to the second decryption verification value.

Rather, Gennaro et al. (US 5,907,618) merely teaches that the receiver performs a validation, depending on the number of copies of the session key K. When the receiver has no independent copy of the session key K, then no validation is necessary. On the other hand, when the receiver has an independent copy of the session key K or when there are multiple sets of key recovery agents, the receiver must ensure that all of the various versions of the session key K agree if the receiver is to fully valid the recovery information. Validation may be done by doubly decrypting the recovery information using the key-encrypting keys KK1 and KK2 and by seeing if the resulting session key K agrees with one independently obtained. Alternatively, validation may be done by doubly encrypting an independently obtained session key K using the key-encrypting keys KK1 and KK2 and by seeing if the result agrees with the recover field. As a further alternative, validation may be done by singly decrypting the recovery field using the key-encrypting key KK1 and singly encrypting the independent session key K using K2, and by seeing if the two operations produces the same value KK2 (K) (col.14, lines 14-41). In other words, Gennaro et al. (US 5,907,618) merely teaches that the receiver verifies the correctness of the session key K by decrypting or/and encrypting the session key K, using the key-encrypting keys KK1 and KK2.

Thus, Applicants submit that Gennaro et al. (US 5,907,618) does not contain any disclosures regarding at least a shared-key recovery apparatus that generates a first decryption verification value and a decryption seed value, as well as a shared-key recovery apparatus that judges whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification

value, and judges that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value.

Thus, the pending claims are clearly distinguished over Gennaro et al. (US 5,907,618).

Based on the foregoing, Applicants submit that neither Gennaro et al. (US 5,937,066) nor Gennaro et al. (US 5,907,618) discloses at least a shared-key recovery apparatus that generates a first decryption verification value and a decryption seed value, as well as a shared-key recovery apparatus that judges whether the first decryption verification value generated from the received first encryption information is identical to the second decryption verification value generated from the decryption seed value, the decryption seed value being generated based on the received second encryption information and the first decryption verification value, and judges that the decryption shared key is identical to the shared key generated in the shared-key generation apparatus when it is judged that the first decryption verification value is identical to the second decryption verification value.

Therefore, Applicants submit that even if one attempted to combine the teaching of Gennaro et al. (US 5,937,066) with Gennaro et al. (US 5,907,618) in the matter suggested by the Examiner, one would fail to arrive at the presently claimed invention, as such a combination would lack, at least, the above combinations of the features of the present invention.

Therefore, Applicants submit that the suggested combination of Gennaro et al. (US 5,937,066) with Gennaro et al. (US 5,907,618) does not render the presently claimed invention obvious, and thus, respectfully request that the U.S.C. § 103(a) rejection be withdrawn.

Accordingly, Applicants respectfully request reconsideration and withdrawal of the outstanding rejection and an indication of the allowability of all the claims pending in the present application in due course.

B. The Examiner has also rejected claims 2, 5-23 and 25-45 under 35 U.S.C §103(a) as being unpatentable over Gennaro et al. (US 5,937,066) in view of Gennaro et al. (US 5,907,618) and Hoffstein et al. (WO/9808323).

As discussed above, Applicants respectfully submit that claims 1, 3, 4, 24, 46, 47, 49 and 50 are patentable over the combination of Gennaro et al. (US 5,937,066) and Gennaro et al. (US 5,907,618). Applicants respectfully submit that Hoffstein et al. fails to cure the deficiencies of Gennaro et al. (US 5,937,066) and Gennaro et al. (US 5,907,618), as discussed above, with respect to independent claims 1, 3, 24, 46, 47, 49 and 50.

Claim 2 depends from independent claim 1, claims 4-23 depend from independent claim 3, and claims 25-45 depend from independent claim 24. Accordingly, Applicants submit that claims 2, 4-23, and 25-45 are patentable at least by virtue of their dependency.

III. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Masato YAMAMICHI et al.

/Kenneth W. Fields/
By: 2008.07.02 17:55:40 -04'00'

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/krg
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 2, 2008